PROCESO DE AUDITORÍA INTERNA Y ETHICAL HACKING

Edwin Rodríguez
frodriguez20@gmail.com
Universidad Piloto de Colombia

Abstract— Today, the information technology (IT) is a key factor in the competitiveness of companies and forms the core of enterprise management. It is essential to evaluate the effectiveness and efficiency with which the companies act as IT is concerned.
IT audit is a process, which is aimed at verifying and ensuring the effectiveness and efficiency of policies and procedures for the implementation and appropriate use of information technology in any field should be broader than simple error detection, you should propose making decisions to correct errors if they exist and how to improve performance. Examination forming an IT Audit covers a range of controls, checks and trials ending in a set of recommendations and an action Plan. It is the development of this Action Plan which sets IT audit apart from than of a traditional audit.

Resumen—Hoy en día, las tecnologías de la información (TI) son un factor clave en la competitividad de las empresas y forman parte del núcleo de la gestión empresarial. Es fundamental evaluar la eficacia y la eficiencia con las que las empresas actúan en lo que TI se refiere.
La Auditoría TI es un proceso, el cual se orienta a la verificación y aseguramiento de la eficacia y de la eficiencia de las políticas y procedimientos establecidos para la implantación y uso adecuado de las Tecnologías de la Información, en cualquier ámbito., debe ser más amplia que la simple detección de errores, debe proponer la toma de decisiones que permitan corregir los errores en caso de que existan y mejorar la forma de actuación. El examen que conforma una auditoría TI abarca una serie de controles, verificaciones y juicios que concluyen en un conjunto de recomendaciones y un plan de acción. Es la elaboración de este Plan de Acción lo que diferencia a la Auditoría TI de lo que sería una auditoría tradicional.

Índice de Términos— PHVA, Caja negra, Caja blanca, Caja gris, Ethical, Hacking, vulnerabilidades, Key logger.

Index Terms — PHVA, Black box, White box, Gray box, Ethical Hacking, vulnerabilities, Key logger.

I. INTRODUCCIÓN

Desarrollar el entendimiento de los procesos generales de la auditoría ti, que permitan la identificación de riesgos a que está sujeto el negocio y el desarrollo de los respectivos controles que minimizarán el impacto de los mismos. Conocer los estándares, controles, normas y guías para la realización de auditorías internas y externas.
También entender y conocer brevemente el objetivo fundamental del ethical hacking (hackeo ético) el cual es explotar las vulnerabilidades existentes en el sistema valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes, aplicaciones web, bases de datos, servidores, con la intención de ganar acceso y demostrar que un sistema es vulnerable, esta información es de gran ayuda al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

II. CONTROL INTERNO

Establecidos en los términos más simples, son mecanismos que garanticen el buen funcionamiento de los procesos dentro de la empresa. Existe Cada sistema y proceso dentro de una empresa con un propósito de negocios específicos. El auditor debe buscar la existencia de riesgos para tal fin, y luego asegurarse de que los controles internos son para mitigar esos riesgos.

Tipos de controles

Los controles pueden ser de carácter preventivo, detective, o reactiva, y pueden tener implementaciones administrativas, técnicas y físicas.

Controles Preventivos.

Los controles preventivos dejan un mal evento suceda. Por ejemplo, lo que requiere un ID de usuario y la contraseña de acceso a un sistema es un control

preventivo. Evita que (teóricamente) que personas no autorizadas accedan al sistema.

Controles de detectives.

Controles Detectives grabar un mal evento después de que haya sucedido. Por ejemplo, el registro de todas las actividades realizadas en un sistema permitirá a revisar los registros en busca de actividades inapropiadas después del evento.

Controles reactivos (aka Controles correctivas).

Controles reactivos caen entre los controles preventivos y de detección. Ellos no impiden que un mal evento se produzca, sino que proporcionan una forma sistemática para detectar cuando esos malos acontecimientos han sucedido y corregir la situación, es por eso que a veces se llaman controles correctivos. Por ejemplo, usted podría tener un sistema antivirus central que detecta.

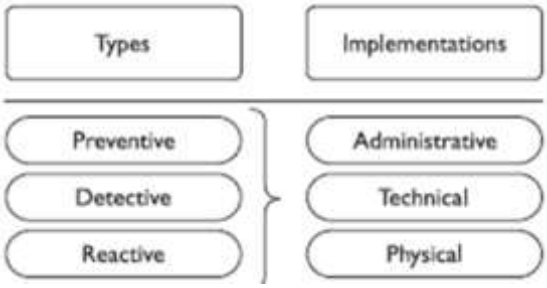

Figura 1. La siguiente figura muestra los tipos de controles internos y su aplicación, [1].

III. ¿QUÉ SE DEBE AUDITAR?

Un plan de auditoría debe enfocar a los auditores en las áreas con mayor riesgo y en áreas donde se puede añadir el máximo valor. Usted debe ser eficiente y eficaz en la forma en que utiliza sus recursos limitados por pasar sus horas de auditoría de TI mirando las áreas de mayor importancia. Esto no se debe hacer tirando arbitrariamente auditorías potenciales fuera del aire; en cambio, debe ser un proceso lógico y metódico que asegura que todas las auditorías potenciales se han consideradas.

IV. ¿POR QUÉ SE DEBEN REALIZAR AUDITORÍAS?

Al igual que cualquier área de la organización, los sistemas de TI deben estar sometidos a controles de calidad y auditoría informática porque las computadoras y los centros de procesamiento de datos son blancos apetecibles para el espionaje, la delincuencia y el terrorismo.

Es importante tener en cuenta que quien realice la auditoría debe ser una persona capacitada.

Las auditorias deben realizarse máximo cada 12 meses, pero es la compañía quien determina el tiempo según sus planes de acción.

V. FASE DE UNA AUDITORÍA

Para realizar una auditoría informática se requiere planear una serie ordenada de acciones y procedimientos específicos, que deben ser ejecutados de forma secuencial, cronológica y ordenada, teniendo en cuenta etapas, eventos y actividades que se requieran para su ejecución que serán establecidos de acuerdo a las necesidades de la empresa. Estos procedimientos se adaptarán de acuerdo al tipo de auditoría de sistemas que se vaya a realizar y con el cumplimiento estricto de las necesidades, técnicas y métodos de evaluación del área de sistematización. Los métodos deben seguirse para la determinación de las herramientas e instrumentos de revisión que serán utilizados en la auditoría, la metodología cubre tres etapas: la primera de planeación, la segunda de ejecución y la tercera del dictamen de la auditoría.

Fase I: Conocimientos del Sistema.

Aspectos Legales y Políticas Internas: Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.

Características del sistema operativo: Organigrama del área que participa en el sistema, Informes de auditoría realizadas anteriormente.

Características de la aplicación de computadora: Manual técnico de la aplicación del sistema, equipos utilizados en la aplicación de computadora.

Fase II: Análisis de las transacciones.

Definición de las transacciones.

Establecer el flujo de los documentos.

Identificar y codificar los recursos que participan en el sistema.

Relación entre transacciones y recursos.

Fase III: Análisis de riesgos y amenazas.

Identificación de riesgos.
Identificación de las amenazas.
Relación entre recursos/amenazas/riesgos.

Fase IV: Análisis de controles.

Codificación de controles.
Relación entre recursos/amenazas/riesgos.
Análisis de cobertura de los controles requeridos.

Fase V: Evaluación de Controles.

Objetivos de la evaluación.
Plan de pruebas de los controles.
Pruebas de controles.
Análisis de resultados de las pruebas.

Fase VI: Informe de Auditoría.

Informe detallado de recomendaciones.
Evaluación de las respuestas.
Informe resumen para la alta gerencia.

Fase VII: Seguimiento de recomendaciones.

Informes del seguimiento.
Evaluación de los controles implantados.

Beneficios.

- Mejora la imagen pública.
- Genera confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad.
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

VI. CICLO PHVA

Mediante este ciclo podremos tener claridad del funcionamiento de los procesos, es decir, la finalidad es saber si todo está funcionando de manera adecuada o si se deben realizar mejoras o ajustes.

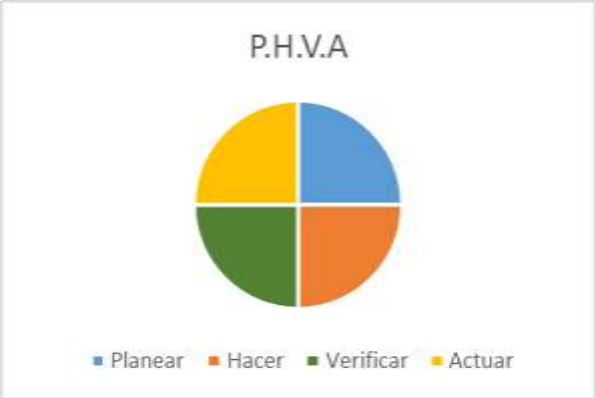

Figura 2. Interpretación grafica del Ciclo PHVA. [2].

A. Planear

Es establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización.

B. Hacer.

Es ejecutar lo planeado, en esta etapa es recomendable hacer pruebas pilotos antes de implantar los procesos definidos. En su desarrollo se puede evidenciar los problemas que se tienen en la implementación, se identifican las oportunidades de mejora y su implementación.

C. Verificar.

En esta etapa comprobamos que se hayan ejecutado los objetivos previstos mediante el seguimiento y medición de los procesos, confirmando que estos estén acorde con las políticas y a toda la planeación inicial.

D. Actuar.

Mediante este paso se realizan las acciones para el mejoramiento del desempeño de los procesos, se corrigen las desviaciones, se estandarizan los cambios, se realiza la formación y capacitación requerida y se define como monitorearlo.

VII. CRITERIOS DE AUDITORÍA

Define que técnicas, normas, políticas, métodos se van a usar.

VIII. ETHICAL HACKING

También conocidos como penetration testing, el proceso utilizado para atacar una organización y descubrir sus vulnerabilidades. Son una Ejecución

controlada de "exploits" de vulnerabilidades encontradas en un análisis de vulnerabilidad previo, consisten en probar los métodos de protección del sistema de información sometiendo el sistema a una situación real.

IX. ¿Por qué hacer ethical hacking?

A través del ethical hacking (es posible detectar el nivel de seguridad interno y externo de los sistemas de información de una organización, esto se logra determinando el grado de acceso que tendría un atacante con intenciones maliciosas a los sistemas informáticos con información crítica.

X. Etapas de un ethical hacking

A. Descubrimiento.

Se usa buscadores, herramientas de análisis de DNS, whois y demás herramientas para obtener información de la víctima. Además, se puede hacer una exploración de metadatos de los documentos, imágenes y otros tipos de archivos que estén al alcance navegando.

B. Enumeración.

Se basa en conseguir direcciones IP del objetivo, nombres de usuarios y contraseñas válidas de su entorno y nombres de servicios y aplicaciones accesibles, y todo aquello que luego pueda ayudar a lanzar un ataque.

C. Análisis de vulnerabilidades.

Se comienza a actuar sobre los sistemas encontrados, se analizan en busca de vulnerabilidades, ya sea en la infraestructura, los sistemas operativos, los servicios disponibles o las aplicaciones existentes.

D. Explotar Vulnerabilidades.

En esta fase se hace la intrusión en el sistema y se obtendrá evidencias de la misma para la posterior documentación o la demostración de que se realizó la intrusión.

E. Reportar y recomendar.

En esta fase genera de forma entendible y accesible todos los hallazgos, Reportar todo lo descubierto sobre los sistemas, realizar informes detallados con evidencia de las intrusiones, realizar una presentación concisa y resumida de resultados, y señalar aquellos puntos que requieren especial importancia o que provocan los problemas más graves o inmediatos.

XI. Tipos de ataque

Existen 2 tipos de ataques.

A. Activos.

Alteran y comprometen la disponibilidad, integridad y autenticidad de la información, afectando los sistemas, redes y aplicaciones informáticas, los ataques usados son: SQL injection.

B. Pasivos.

Se Estos no alteran ni modifican los sistemas o redes, solo obtiene y compromete la confidencialidad, un tipo de ataque es, sniffing de red.

Algunas de las técnicas usadas:

A. Denegación de servicio.

También llamado ataque DoS (Denial of Service) o DDoS (de Distributed Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

B. Identificación de contraseña por fuerza bruta.

Consiste en adivinar repetitivamente la contraseña y corroborar contra un hash criptográfico existente de la contraseña.

La herramienta más usada para este tipo de ataque es hydra.

¿Con qué protocolos funciona hydra?

Hydra es una herramienta de penetración para el testing muy versátil que ha sido usada con la mayoría de sistemas de protocolos de seguridad modernos. Algunos ejemplos de ello son:

Cisco.
Cisco-enable.
HTTPS-form-get.
MySQL.
SSH2.
SIP.

FTP.
Oracle-listener.
MSSQL.
IMAP.

C. Explotación de vulnerabilidades.

Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. Ejemplos de comportamiento erróneo: Acceso de forma no autorizada, toma de control de un sistema de cómputo, consecución privilegios no concedidos lícitamente, consecución de ataques de denegación de servicio.

D. Phising.

También conocido como suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

E. Spoofing.

En términos de seguridad de redes hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
Se pueden clasificar los ataques de spoofing, en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

F. Ingeniería social.

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema está solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (se pronuncia igual que "fishing", pesca).

XII. METODOLOGÍAS ETHICAL HAKING

Las mejores metodologías y técnicas utilizadas en el mundo del Ethical Hacking.

A. OSSTMM (Open-Source Security Testing Methodology Manual).

Metodología que propone un proceso de evaluación de una serie de áreas que refleja de manera fiel los niveles de seguridad presentes en la infraestructura como parte de un trabajo secuencial la metodología OSSTMM consta de 6 ítems los cuales comprenden todo sistema actual, estos son:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las comunicaciones.
- Seguridad inalámbrica.
- Seguridad Física.

B. ISSAF (Information Systems Security Assessment Framework).

Marco metodológico de trabajo desarrollado por la OISSG que permite clasificar la información de la evaluación de seguridad en diversos dominios usando diferentes criterios de prueba. Algunas de las características más representativas de ISSAF son:

- Brinda medidas que permiten reflejar las condiciones de escenarios reales para las evaluaciones de seguridad.
- Esta metodología se encuentra principalmente enfocada en cubrir los procesos de seguridad y la evaluación de los mismos para así obtener un panorama completo de las vulnerabilidades existentes.
- Permite el desarrollo de matriz de riesgo para verificar la efectividad en la implementación de controles.

C. OWASP (Open web application security Project).

Metodología de pruebas enfocada en la seguridad de aplicaciones, El marco de trabajo descrito en este

documento pretende alentar a las personas a evaluar y tomar una medida de la seguridad a través de todo el proceso de desarrollo. Así, pueden relacionar los costes de un software inseguro al impacto que tiene en su negocio, y de este modo gestionar decisiones de negocio apropiadas (recursos) para la gestión del riesgo, algunas de las características más representativas de OWASP son:

- Pruebas de firma digital de aplicaciones Web.
- Comprobaciones del sistema de autenticación.
- Pruebas de Cross Site Scripting.
- Inyección XML.
- Inyección SOAP.
- HTTP Smuggling.
- Sql Injection.
- LDAP Injection.
- Polución de Parámetros.
- Cookie Hijacking.
- Cross Site Request Forgery.

D. CEH (Certified ethical hacking).

Metodología de pruebas de seguridad desarrollada por el International Council of Electronic Commerce Consultants (EC-Council) algunas de las fases enunciadas en esta metodología son:

- Obtención de Información.
- Obtención de acceso.
- Enumeración.
- Escala de privilegios.
- Reporte.

E. Offensive security.

Metodología líder a nivel mundial para el desarrollo de pruebas de penetración y estudios de seguridad, la metodología contempla principalmente los métodos para el desarrollo de estudios de seguridad enfocados en seguridad ofensiva y teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades, las principales ventajas de adoptar este marco metodológico son:

- Enfoque sobre la explotación real de las plataformas.
- Enfoque altamente intrusivo.
- Enfoque orientado a resultados tangibles y no a estadísticas generadas por herramientas).

XIII. HERRAMIENTAS DE ETHICAL HACKING

Dentro de las metodologías utilizadas en el ethical hacking, se utilizan entre otras las siguientes herramientas:

A. Nmap.

Herramienta estándar usada mundialmente por miles de consultores en el mundo, algunas de las características más representativas de nmap son:

- Escaneo de Puertos.
- Escaneo de servicios.
- Escaneo de vulnerabilidades.
- Escaneo de redes.
- Escaneo por scripts.

B. Ncat.

Utilidad que tiene entre otras las siguientes características:

- Redirección TCP y UDP.
- Escáner de puertos.
- Service binding.
- Soporte para SSL.
- Soporte para Proxys.

C. Ncrack

Herramienta para cracking de autenticación de alta velocidad, algunas de las características de esta herramienta son:

- Soporte para RDP.
- Soporte para SSH.
- Soporte para SMB.
- Soporte para VNC.
- Soporte para VNC.
- Soporte para FTP.
- Soporte para Telnet.

D. Metasploit framework.

Framework de explotación desarrollado en Ruby usado ampliamente a nivel mundial por consultores en seguridad, algunas de las características destacadas del framework son:

- Amplia base de datos de exploits.
- Diversos Payloads de ejecución.
- Soporte para post-explotación.
- Permite atacar diferentes plataformas.

E. Matelgo.

Herramienta ampliamente usada mundialmente para

el desarrollo de etapas de obtención de información. Los resultados proporcionados por maltego pueden ser usados en diferentes fases de un ataque.

F. Yersinia.

Herramienta de red que permite tomar ventaja de los diferentes tipos de vulnerabilidades en diferentes protocolos de red, con yersinia se pueden realizar ataques contra los siguientes protocolos.

- Spanning Tree Protocol (STP).
- Cisco Discovery Protocol (CDP).
- Dynamic Trunking Protocol (DTP).
- Dynamic Host Configuration Protocol (DHCP).
- Hot Standby Router Protocol (HSRP).
- IEEE 802.1Q.
- IEEE 802.1X.
- Inter-Switch Link Protocol (ISL).
- VLAN Trunking Protocol (VTP).

G. Dsniff.

Sniffer usado ampliamente en pruebas de penetración con capacidades interceptación de tráfico de red. Adicionalmente dsniff incluye las herramientas arpspoof, dnsspoof y macof.

H. Ettercap.

Sniffer de red con capacidades de realizar ataques del tipo Man In The Middle y con un amplio soporte de plugins.

I. Ike-Scan.

Herramienta especializada para realizar ataques sobre firewalls, concentradores de VPN's y dispositivos que usen el protocolo IKE.

J. Nessus.

Scanner de vulnerabilidades conocido ampliamente a nivel mundial con soporte de scripts personalizados mediante el uso de Nessus Attack Scripting Language NASL.
Algunas de las características más representativas de Nessus son:

- Permanente actualización.
- Reportes de riesgos con categorización del mismo.
- Posibilidad de escanear máquinas de forma simultánea.
- Posibilidad de integración con otras herramientas como metasploit y nmap.

K. Social engineering toolkit.

Herramienta líder mundialmente para el desarrollo de vectores de ataque relacionados con ingeniería social, incluyendo Phising, Credential Harvesting y otros vectores de ataque dirigidos a explotar vulnerabilidades humanas en usuarios y administradores.

L. Backtrack5.

Principal distribución cuyo propósito específico es la seguridad en redes, considerada actualmente la distribución más avanzada de Linux diseñada con un propósito específico de seguridad, desarrollada por profesionales de la seguridad y en total alineación con las metodologías descritas anteriormente, cuenta de forma nativa con más de 300 herramientas de seguridad incorporadas.

XIV. TÉCNICA PARA CREAR DICCIONARIO E IDENTIFICAR CONTRASEÑAS.

Herramienta para cracking de autenticación de alta velocidad, algunas de las características de esta herramienta son:

A. Identifica la red o la máquina que se va a vulnerar.

B. Con esta técnica crearemos un diccionario usando la herramienta crunch la cual se encuentra disponible en kali linux. En este ejemplo vamos a crear el diccionario utilizando los caracteres 1234567890 las contraseñas generadas tendrán mínimo 8 caracteres y máximo 8 caracteres y se guardaran en el directorio llamado articulo-ethical. Para ello ejecutamos el comando: crunch 8 8 1234567890 > articulo-ethical.

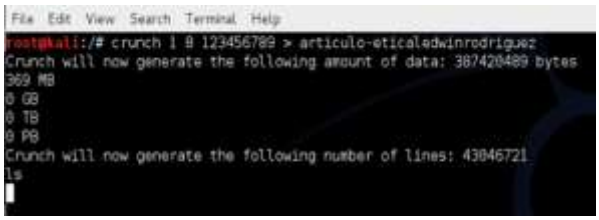

Figura 3. Esta figura muestra cómo se genera un diccionario. [3].

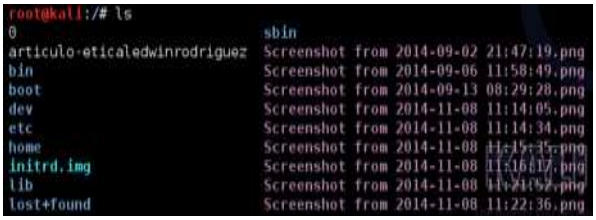

Figura 4. Esta figura evidencia la creación del diccionario. [4]

C. Haciendo uso de Zenmap se indentifican los equipos y dispositivos evidenciando los puerto que pueden ser vulnerables.

Figura 5. Esta figura evidencia el uso de la aplicación Zenmap mediante el sistema operativo Kali-Linux. [5].

D. Se deberá establecer una conexión SHH.

Figura 6. Comando para establecer conexión SHH, Taller ethical hacking. [6].

E. Teniendo claro los dispositivos que se deben atacar, se realizar un análisis de vulnerabilidad por medio de la herramienta Nessus.

Figura 7. Evidencia de resultado de vulnerabilidades encontradas. [7].

F. La corporación Mitre pone a disposición un diccionario Público de vulnerabilidades y les asigna un código el cual ha sido adoptado como estándar incluso para normas locales Como la circular 052 de la Superintendencia Financiera de Colombia.

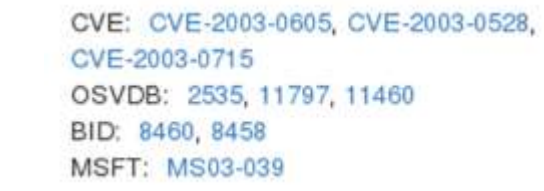

Figura 8. Evidencia el CVE de la vulnerabilidad. [8].

Figura 9. Evidencia de la vulnerabilidad encontrada y validad en la paginas de mitre, [9].

G. Vulnerabilidad: UnreallRCd Backdoor Detection Descripción: Esta puerta trasera permitía a cualquier persona ejecutar diversos comandos con los privilegios del usuario ejecutando ircd. La puerta trasera era ejecutada sin importar las restricciones del usuario.

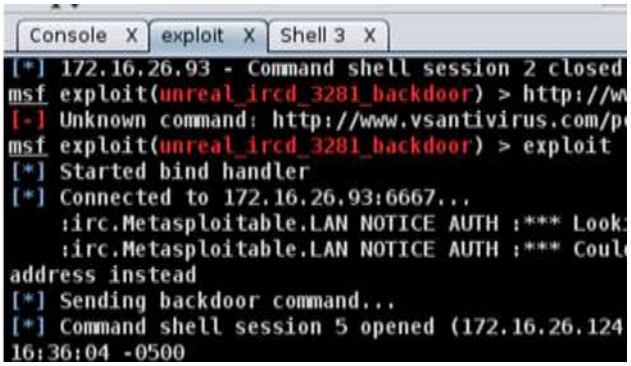

Figura 10. Evidencia de explotación backdoor, muestra la sesión abierta. [10].

H. Exiten diversas herramientas para realizar ataques o explotar vulnerabilidades, entre ellas destacamos ARMITAGE, herramienta que viene integrada en el sistema operativo, Kali – Linux, por medio de ella se puede tomar pantallazos de un computador, asi como tomar remotamente y muchas otras funciones.

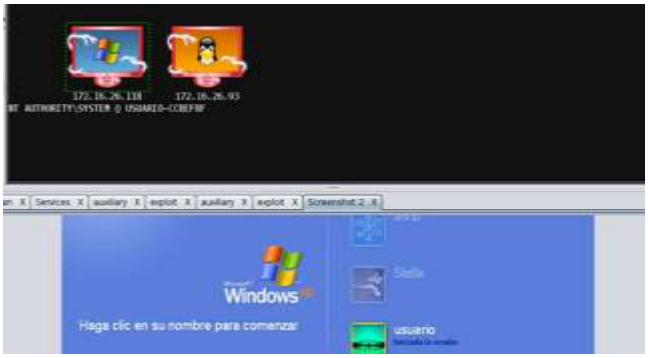

Figura 11. Uso de armitage para tomar pantallazo o print screen de una computadora. [11].

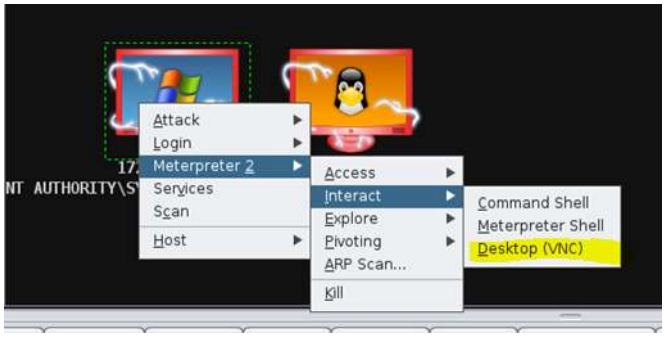

Figura 12. Evidencia de acceso o control remoto mediante armitage haciendo uso de una vulnerabilidad presentada en la aplicación VNC. [12].

Figura 13. Muestra cómo fueron extraídos los hash de usuarios mediante armitage. [13].

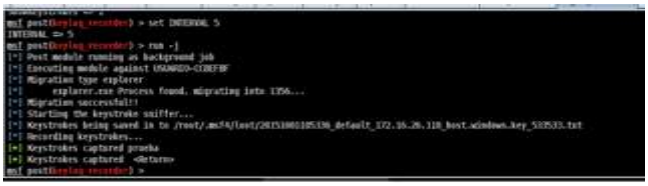

Figura 14. Revela cómo se puede hacer la intromisión de un keylogger. [14].

XV. CONCLUSIONES

A. Es sumamente importante realizar auditorías en informática, se debe comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además se debe evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

B. La auditoría en informática es de vital para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software). Queda claro que existen herramientas que ayudan a tener un control sobre las vulnerabilidades que puedan existir en un entorno laboral.

C. Los procesos de ethical hacking, verifican y evalúan la seguridad tanto física como lógica, de la red, de los sistemas de información, de la configuración de los servidores, de las bases de datos, de las aplicaciones, de los elementos para mitigar el impacto de amenazas e incluso la concientización de lasI personas y empleados en un ambiente empresarial.

REFERENCIAS

[1] CHRIS, Davis, MIKE Schiller, KEVIN Wheeler. 2011. IT Auditing Using Controls to Protect Information Assets, 2nd Edition.
[2] Curso auditor interno ISO27001.
[3] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[4] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[5] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia
[6] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[7] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[8] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[9] https://cve.mitre.org/
[10] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia.
[11] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia
[12] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia
[13] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia
[14] Edwin Rodríguez, Taller ethical hacking. Universidad piloto de Colombia
[15] CHRIS, Davis, MIKE Schiller, KEVIN Wheeler. 2011. IT Auditing Using Controls to Protect Information Assets, 2nd Edition.
[16] Alejandro, Reyes. Unam Cert, 2010. http://www.seguridad.unam.mx/descarga.dsc?arch=2776.
[17] SANCHEZ, YULI. GERENCIA.COM, 2014, http://www.gerencie.com/ciclo-phva.html.
[18] RENAN, Quevedo, 2015. Seminario ethical hacking.
[19] CAMPUS, Party, 2010. https://infow.wordpress.com/2010/08/04/fases-de-un-test-de-penetracion/.

[20] CYBERSEGURIDAD.NET, 2015. http://cyberseguridad.net/index.php/455-las-fases-de-un-test-de-penetracion-pentest-pentesting-i.
[21] ISAZA, Miguel, 2013, http://seguridadinformaticahoy.blogspot.com.co/2013/02/metodologias-y-herramientas-de-ethical.html.
[22] Https://es.wikipedia.org/wiki/.